

**IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF GEORGIA**

CHRIS BROWN, MARIUS )  
ANDREICA, DEREK )  
BAUMGARDNER, TIM )  
BORLAND, JAMIE BENSON, )  
RUSS BENSON, VAL )  
CHEKMAZOV, PETER COOKE, )  
MICHAEL ERICKSON, EMILY )  
GREEN, WALTER HINCK, )  
KATHLEEN HOLLY, JOSHUA )  
IRON WING, GARY JAETZOLD, )  
PATRICIA A. KOLLER, )  
MARGARET McCABLE, )  
DANIEL E. OBERST, JAMES )  
PEACOCK, RICHARD )  
POLIGIAN, CHAD ROOFENER, )  
CORREE ROOFENER, )  
ELISABETA SZEKELY, KELLIE )  
WILLIAMS, and MICHAEL JAY )  
WILLIAMS, individually and on )  
behalf of all others similarly )  
situated, )  
  
Plaintiffs, )  
  
v. )  
  
EQUIFAX INC. and TRUSTEDID, )  
INC., )  
  
Defendants. )

Civil Action No.: 1:17-cv-03449-SCJ

**CLASS ACTION**

**JURY TRIAL DEMANDED**

**AMENDED CLASS ACTION COMPLAINT**

**TABLE OF CONTENTS**

NATURE OF THE ACTION .....1

JURISDICTION AND VENUE .....4

PARTIES.....5

FACTUAL BACKGROUND.....14

    The Equifax Security Breach.....15

    Equifax’s Prior Data Security Offenses.....18

    Security Breaches Lead to Identity Theft .....19

    The Monetary Value of Privacy Protections and Private Information.....20

    Damages Sustained by Plaintiffs and the Other Class Members .....23

CLASS ACTION ALLEGATIONS .....24

CLAIMS.....28

    I. Willful Failure to Comply with the Fair Credit Reporting Act.....28

    II. Negligent Failure to Comply with the Fair Credit Reporting Act .....30

    III. Negligence .....32

    IV. Alaska Unfair Trade Practices and Consumer Protection Act .....34

    V. Alaska Personal Information Protection Act.....36

    VI. District of Columbia Consumer Protection Procedures Act .....37

    VII. District of Columbia Consumer Security Breach Notification Act .....38

VIII.	Florida Deceptive and Unfair Trade Practices Act .....	39
IX.	Illinois Consumer Fraud Act .....	41
X.	Illinois Personal Information Protection Act .....	42
XI.	Kansas Fair Credit Reporting Act .....	43
XII.	Kansas Consumer Protection Act.....	45
XIII.	Kentucky Consumer Protection Act.....	47
XIV.	Maine Fair Credit Reporting Act.....	48
XV.	Maryland Consumer Protection Act.....	50
XVI.	Maryland Personal Information Protection Act .....	52
XVII.	Maryland Consumer Credit Reporting Agencies Act .....	53
XVIII.	Maryland Social Security Number Privacy Act.....	55
XIX.	Massachusetts Fair Credit Reporting Act.....	56
XX.	Massachusetts Consumer Protection Act .....	58
XXI.	New Hampshire Fair Credit Reporting Act.....	60
XXII.	New Hampshire Consumer Protection Act .....	62
XXIII.	New Hampshire Notice of Security Breach Act .....	63
XXIV.	North Carolina Unfair and Deceptive Trade Practices Act.....	64
XXV.	North Carolina Protection from Security Breaches Act.....	66
XXVI.	New Mexico Unfair Practices Act.....	67

XXVII. New Mexico Privacy Protection Act.....68

XXVIII. Ohio Consumer Sales Practices Act.....69

XXIX. Oregon Unfair Trade Practices Act .....71

XXX. Oregon Consumer Identity Theft Protection Act .....72

XXXI. Texas Deceptive Trade Practices-Consumer Protection Act .....74

XXXII. Virginia Breach of Personal Information Notification Statute .....76

XXXIII. Washington Fair Credit Reporting Act .....76

XXXIV. Washington Consumer Protection Act.....79

XXXV. Washington Data Breach Notification Statute .....80

DEMAND FOR JURY TRIAL .....81

REQUEST FOR RELIEF .....81

Plaintiffs Chris Brown, Marius Andreica, Derek Baumgardner, Tim Borland, Jamie Benson, Russ Benson, Val Chekmazov, Peter Cooke, Michael Erickson, Emily Green, Walter Hinck, Kathleen Holly, Joshua Iron Wing, Gary Jaetzold, Patricia A. Koller, Margaret McCable, Daniel E. Oberst, James Peacock, Richard Poligian, Chad Roofener, Corree Roofener, Elisabeta Szekely, Kellie Williams, and Michael Jay Williams (“Plaintiffs”), individually and on behalf of all others similarly situated, upon personal knowledge of the facts pertaining to themselves and on information and belief as to all other matters, by and through undersigned counsel, hereby bring this Amended Class Action Complaint against defendants Equifax Inc. (“Equifax”) and TrustedID, Inc. (“TrustedID”) (collectively, “Defendants”).

### **NATURE OF THE ACTION**

1. Plaintiffs bring this class action against Equifax for its failure to secure and safeguard the private information of approximately 143 million Americans.

2. On July 29, 2017, Equifax discovered unauthorized access to databases storing the confidential and private consumer information of millions of U.S. consumers.

3. On September 7, 2017, Equifax publicly announced that, due to a vulnerability in its systems, its files were accessed by criminals for at least the period of mid-May through July of 2017 (“Security Breach”). The information accessed includes names, social security numbers, birth dates, addresses, and driver’s license numbers, in addition to credit card numbers for some consumers and other documents containing personal identity information (“Private Information”).

4. Plaintiffs’ and Class members’ Private Information was accessed and stolen by hackers in the Security Breach.

5. The hackers exploited a widely known vulnerability that had a fix. Equifax has identified the vulnerability known as Apache Struts CVE-2017-5638. The bug was patched on March 6, 2017, and an update made available shortly thereafter. Knowing the patch was available, hackers scoured the web for systems that had yet to install the update. Equifax failed to update its systems to cure the fix.

6. Equifax’s security failures enabled and facilitated the criminals’ access, obtainment, theft, and misuse of Plaintiffs’ and Class members’ Private Information. Unauthorized persons gained access to Equifax’s databases through vulnerabilities in its security and executed commands that caused the system to

transmit to the unauthorized persons electronic data comprising millions of Americans' Private Information. Equifax's security failures also put Plaintiffs and the other Class members at serious, immediate, and ongoing risk of identity theft, and additionally, will cause costs and expenses to Plaintiffs and the other Class members attributable to responding, identifying, and correcting damages that are reasonably foreseeable as a result of Equifax's willful or negligent conduct.

7. The Security Breach was caused and enabled by Equifax's knowing violation of its obligations to secure consumer information. Equifax failed to comply with security standards and allowed the Private Information of millions collected by Equifax to be compromised by cutting corners on security measures that could have prevented or mitigated the Security Breach.

8. TrustedID negligently failed to provide the TrustedID Premier services to consumers. As a result of TrustedID's negligence, consumers will be further harmed.

9. Accordingly, Plaintiffs, on behalf of themselves and all others similarly situated, assert claims for violation of the Fair Credit Reporting Act, violations of their respective State consumer protection statutes and data breach statutes, and negligence. Plaintiffs seek monetary damages, punitive damages,

statutory damages, and injunctive relief, and all other relief as authorized in equity and by law.

### **JURISDICTION AND VENUE**

10. The Court has subject matter jurisdiction under 28 U.S.C. § 1331 because Plaintiffs' Fair Credit Reporting Act claims arise under the laws of the United States. The Court has supplemental jurisdiction over the remaining claims under 28 U.S.C § 1367.

11. The Court also has jurisdiction over Plaintiffs' state law claims under 28 U.S.C. § 1332(d)(2), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendants' citizenship, and (c) the matter in controversy exceeds \$5,000,000, exclusive of interest and costs.

12. The Court has personal jurisdiction over Equifax Inc. because Equifax Inc. is a Georgia corporation headquartered in Atlanta, Georgia.

13. The Court has personal jurisdiction over TrustedID, Inc. because the claims against TrustedID, Inc. arise from TrustedID, Inc.'s contacts with the State of Georgia.



14. Venue is proper in this District under 28 U.S.C. §§ 1391(b)(2) because a substantial part of the events and omissions giving rise to these claims occurred in this District.

### **PARTIES**

15. Russ Benson resides in and is a citizen of the State of Alaska. After learning of the Security Breach, Benson used a tool on Equifax's website to determine whether his Private Information was affected. Using this tool, Benson determined that his private information was affected by the Security Breach. As a result of the Security Breach, Benson suffered from the deprivation of the value of his Private Information and has incurred and will incur costs and expenditures to protect himself from identity theft.

16. Jamie Benson resides in and is a citizen of the State of Alaska. After learning of the Security Breach, Benson used a tool on Equifax's website to determine whether her Private Information was affected. Using this tool, Benson determined that her private information was affected by the Security Breach. As a result of the Security Breach, Benson suffered from the deprivation of the value of her Private Information and has incurred and will incur costs and expenditures to protect herself from identity theft.

17. Emily Green resides in and is a citizen of the State of Florida. After learning of the Security Breach, Green used a tool on Equifax's website to determine whether her Private Information was affected. Using this tool, Green determined that her private information was affected by the Security Breach. As a result of the Security Breach, Green suffered from the deprivation of the value of her Private Information and has incurred and will incur costs and expenditures to protect herself from identity theft.

18. Kathleen Holly resides in and is a citizen of the District of Columbia. After learning of the Security Breach, Holly used a tool on Equifax's website to determine whether her Private Information was affected. Using this tool, Holly determined that her private information was affected by the Security Breach. As a result of the Security Breach, Holly suffered from the deprivation of the value of her Private Information and has incurred and will incur costs and expenditures to protect herself from identity theft.

19. Walter Hinck resides in and is a citizen of the State of Florida. After learning of the Security Breach, Hinck used a tool on Equifax's website to determine whether his Private Information was affected. Using this tool, Hinck determined that his private information was affected by the Security Breach. As a result of the Security Breach, Hinck suffered from the deprivation of the value of

his Private Information and has incurred and will incur costs and expenditures to protect himself from identity theft.

20. Val Chekmazov resides in and is a citizen of the State of Illinois. After learning of the Security Breach, Chekmazov used a tool on Equifax's website to determine whether his Private Information was affected. Using this tool, Chekmazov determined that his private information was affected by the Security Breach. As a result of the Security Breach, Chekmazov suffered from the deprivation of the value of his Private Information and has incurred and will incur costs and expenditures to protect himself from identity theft.

21. Joshua Iron Wing resides in and is a citizen of the State of Kansas. After learning of the Security Breach, Iron Wing used a tool on Equifax's website to determine whether his Private Information was affected. Using this tool, Iron Wing determined that his private information was affected by the Security Breach. As a result of the Security Breach, Iron Wing suffered from the deprivation of the value of his Private Information and has incurred and will incur costs and expenditures to protect himself from identity theft.

22. Patricia A. Koller resides in and is a citizen of the State of Kentucky. After learning of the Security Breach, Koller used a tool on Equifax's website to determine whether her Private Information was affected. Using this tool, Koller

determined that her private information was affected by the Security Breach. As a result of the Security Breach, Koller suffered from the deprivation of the value of her Private Information and has incurred and will incur costs and expenditures to protect herself from identity theft.

23. Daniel E. Oberst resides in and is a citizen of the State of Kentucky. After learning of the Security Breach, Oberst used a tool on Equifax's website to determine whether his Private Information was affected. Using this tool, Oberst determined that his private information was affected by the Security Breach. As a result of the Security Breach, Oberst suffered from the deprivation of the value of his Private Information and has incurred and will incur costs and expenditures to protect himself from identity theft.

24. Richard Poligian resides in and is a citizen of the State of Massachusetts. After learning of the Security Breach, Poligian used a tool on Equifax's website to determine whether his Private Information was affected. Using this tool, Poligian determined that his private information was affected by the Security Breach. As a result of the Security Breach, Poligian suffered from the deprivation of the value of his Private Information and has incurred and will incur costs and expenditures to protect himself from identity theft.

25. Derek Baumgardner resides in and is a citizen of the State of Maryland. After learning of the Security Breach, Baumgardner used a tool on Equifax's website to determine whether his Private Information was affected. Using this tool, Baumgardner determined that his private information was affected by the Security Breach. As a result of the Security Breach, Baumgardner suffered from the deprivation of the value of his Private Information and has incurred and will incur costs and expenditures to protect himself from identity theft.

26. Margaret McCable resides in and is a citizen of the State of New Hampshire. After learning of the Security Breach, McCable used a tool on Equifax's website to determine whether her Private Information was affected. Using this tool, McCable determined that her private information was affected by the Security Breach. As a result of the Security Breach, McCable suffered from the deprivation of the value of her Private Information and has incurred and will incur costs and expenditures to protect herself from identity theft.

27. Marius Andreica resides in and is a citizen of the State of New Hampshire. After learning of the Security Breach, Andreica used a tool on Equifax's website to determine whether his Private Information was affected. Using this tool, Andreica determined that his private information was affected by the Security Breach. As a result of the Security Breach, Andreica suffered from the

deprivation of the value of his Private Information and has incurred and will incur costs and expenditures to protect himself from identity theft.

28. Elisabeta Szekely resides in and is a citizen of the State of New Mexico. After learning of the Security Breach, Szekely used a tool on Equifax's website to determine whether her Private Information was affected. Using this tool, Szekely determined that her private information was affected by the Security Breach. As a result of the Security Breach, Szekely suffered from the deprivation of the value of her Private Information and has incurred and will incur costs and expenditures to protect herself from identity theft.

29. Chris Brown resides in and is a citizen of the State of North Carolina. After learning of the Security Breach, Brown used a tool on Equifax's website to determine whether his Private Information was affected. Using this tool, Brown determined that his private information was affected by the Security Breach. As a result of the Security Breach, Brown suffered from the deprivation of the value of his Private Information and has incurred and will incur costs and expenditures to protect himself from identity theft.

30. Peter Cooke resides in and is a citizen of the State of Maine. After learning of the Security Breach, Cooke used a tool on Equifax's website to determine whether his Private Information was affected. Using this tool, Cooke

determined that his private information was affected by the Security Breach. As a result of the Security Breach, Cooke suffered from the deprivation of the value of his Private Information and has incurred and will incur costs and expenditures to protect himself from identity theft.

31. Kellie Williams resides in and is a citizen of the State of Ohio. After learning of the Security Breach, Williams used a tool on Equifax's website to determine whether her Private Information was affected. Using this tool, Williams determined that her private information was affected by the Security Breach. As a result of the Security Breach, Williams suffered from the deprivation of the value of her Private Information and has incurred and will incur costs and expenditures to protect herself from identity theft.

32. Michael Jay Williams resides in and is a citizen of the State of Ohio. After learning of the Security Breach, Williams used a tool on Equifax's website to determine whether his Private Information was affected. Using this tool, Williams determined that his private information was affected by the Security Breach. As a result of the Security Breach, Williams suffered from the deprivation of the value of his Private Information and has incurred and will incur costs and expenditures to protect himself from identity theft.

33. Corree Roofener resides in and is a citizen of the State of Oregon. After learning of the Security Breach, Roofener used a tool on Equifax's website to determine whether her Private Information was affected. Using this tool, Roofener determined that her private information was affected by the Security Breach. As a result of the Security Breach, Roofener suffered from the deprivation of the value of her Private Information and has incurred and will incur costs and expenditures to protect herself from identity theft.

34. Chad Roofener resides in and is a citizen of the State of Oregon. After learning of the Security Breach, Roofener used a tool on Equifax's website to determine whether his Private Information was affected. Using this tool, Roofener determined that his private information was affected by the Security Breach. As a result of the Security Breach, Roofener suffered from the deprivation of the value of his Private Information and has incurred and will incur costs and expenditures to protect himself from identity theft.

35. Gary Jaetzold resides in and is a citizen of the State of Texas. After learning of the Security Breach, Jaetzold used a tool on Equifax's website to determine whether his Private Information was affected. Using this tool, Jaetzold determined that his private information was affected by the Security Breach. As a result of the Security Breach, Jaetzold suffered from the deprivation of the value of



his Private Information and has incurred and will incur costs and expenditures to protect himself from identity theft.

36. Michael Erickson resides in and is a citizen of the Commonwealth of Virginia. After learning of the Security Breach, Erickson used a tool on Equifax's website to determine whether his Private Information was affected. Using this tool, Erickson determined that his private information was affected by the Security Breach. As a result of the Security Breach, Erickson suffered from the deprivation of the value of his Private Information and has incurred and will incur costs and expenditures to protect himself from identity theft.

37. James Peacock resides in and is a citizen of the State of Washington. After learning of the Security Breach, Peacock used a tool on Equifax's website to determine whether his Private Information was affected. Using this tool, Peacock determined that his private information was affected by the Security Breach. As a result of the Security Breach, Peacock suffered from the deprivation of the value of his Private Information and has incurred and will incur costs and expenditures to protect himself from identity theft.

38. Tim Borland resides in and is a citizen of the State of Minnesota. After learning of the Security Breach, Borland used a tool on Equifax's website to determine whether his Private Information was affected. Using this tool, Borland

determined that his private information was affected by the Security Breach. As a result of the Security Breach, Borland suffered from the deprivation of the value of his Private Information and has incurred and will incur costs and expenditures to protect himself from identity theft.

39. Equifax Inc. is a nationwide consumer reporting agency and purveyor of credit monitoring and identity theft protection services. Equifax is a Georgia corporation headquartered in Atlanta, Georgia.

40. TrustedID, Inc. is a Delaware corporation headquartered in Palo Alto, California.

### **FACTUAL BACKGROUND**

41. Equifax is in the business of collecting, assessing, and maintaining the Private Information of approximately 800 million consumers around the world in order to sell this information to third parties in the form of consumer credit reports, consumer insurance reports, or consumer demographic or analytics information. It also sells credit protection and identity theft monitoring services to consumers.

42. In the years preceding Equifax's announcement of the Security Breach, several entities storing large quantities of consumer data were the subject of massive security breaches, including health insurer Anthem, Yahoo, Equifax's competitor, Experian, and many others. Equifax knew or should have known that

the Private Information contained in its databases was a prime target for hackers. In fact, it makes many millions of dollars in profits convincing Americans to buy its credit protection and identity theft monitoring services to guard against such breaches and the damages they cause. Despite this, Equifax failed to take adequate steps to secure its systems.

43. Given the nature of Equifax's business, its databases are natural targets for criminals bent on engaging in identity theft and other fraudulent activity.

***The Equifax Security Breach***

44. On September 7, 2017, Equifax announced that its systems were compromised by cybercriminals, reportedly impacting approximately 143 million U.S. consumers. The Security Breach began in mid-May, 2017, and was not detected by Equifax for several months. Equifax admits the Security Breach arose from a "U.S. website application vulnerability" in its systems.

45. Equifax failed to update its systems to patch a known vulnerability in the Apache Struts framework, an open source code commonly used by websites where users complete online forms.

46. On March 7, 2017, Apache disclosed a vulnerability in its software that could allow a hacker to execute commands remotely on a targeted system.

Apache assessed the security rating as “critical,” and strongly advised users to implement a patch addressing the vulnerability. On the heels of the publication and the patch, hackers scoured for ways to exploit entities that had not installed the update.

47. The U.S. Computer Emergency Readiness Team, a part of the Department of Homeland Security, published a notification about the vulnerability, as well.

48. Equifax failed to adequately address the known vulnerabilities presented and addressed in the update and failed to take adequate measures after the publication of the vulnerability to ensure that its systems were secured and had not been infiltrated or penetrated through the vulnerability.

49. As a result of Equifax’s failures, unauthorized persons manipulated Equifax’s security vulnerabilities to access databases of consumer information. Equifax’s systems transmitted to the unauthorized persons during a period of time of over two months without Equifax detecting or limiting the infiltration.

50. After Equifax discovered the Security Breach on July 29, 2017, it waited more than one month before it began notifying impacted consumers on September 7, 2017.

51. In response to the breach, Equifax set up a website, “equifaxsecurity2017.com.” On this website, Equifax offers one year of TrustedID Premier services, whether or not a consumer’s information was included in the breach.

52. By using the domain name “equifaxsecurity2017.com” instead of creating a page on a recognizable domain such as “equifax.com,” Equifax exposed consumers to phishing scams aimed at stealing consumer information. To lampoon this poor security decision, a website deriding Equifax was created at “securityequifax2017.com.” Equifax itself fell for the trick, tweeting a hyperlink to the incorrect “securityequifax2017.com” URL from its official Twitter account on numerous occasions.

53. Many consumers are complaining that the enrollment process for the promised TrustedID Premier service is not functioning at all.<sup>1</sup> Meanwhile, consumers unable to enroll in this service are forced to look elsewhere for protection due to Equifax and TrustedID, Inc.’s negligent failure to provide the promised service.

---

<sup>1</sup> See Michelle Singletary, *Equifax Says It’s Overwhelmed. Its Customers Say They are Getting the Runaround*, The Washington Post, [https://www.washingtonpost.com/news/get-there/wp/2017/09/19/equifax-says-its-overwhelmed-its-customers-say-they-are-getting-the-runaround/?utm\\_term=.ce6ba9ec774d](https://www.washingtonpost.com/news/get-there/wp/2017/09/19/equifax-says-its-overwhelmed-its-customers-say-they-are-getting-the-runaround/?utm_term=.ce6ba9ec774d) (last visited Sept. 22, 2017).

54. The consumer information compromised in the Security Breach includes, but is not limited to, names, Social Security numbers, birth dates, addresses, driver's license numbers, credit card numbers, and documents containing personal identity information—all information that is now in the hands of criminals.

***Equifax's Prior Data Security Offenses***

55. Equifax is a repeat offender when it comes to data breaches and data security deficiencies. In April 2013 and January 2014, Equifax reported to governmental authorities that as a result of data security deficiencies, an IP address operator was able to obtain credit reports using sufficient personal information to meet Equifax's identity verification process.

56. In January 2017, Equifax was forced to confess to a data leak in which credit information of customers at credit security partner LifeLock had been exposed to another user of LifeLock's online portal.

57. In 2016 a security research found a common vulnerability known as cross-site scripting (XSS) on the main Equifax website.

58. In another incident, from April 2016 to March 2017, hackers exploited Equifax's inadequate data security and gained unauthorized access to Equifax's payroll subsidiary TALX, absconding with W2 tax data of employees of Equifax's

clients' employees. Although Equifax made assurances that it would discontinue the unsecure practices, in May 2017, it was revealed that in fact it had not, and that the same vulnerabilities were able to be exploited.

59. Through these incidents, Equifax has shown a disdain for the privacy of the valuable and personal information it collects of millions of Americans without their knowledge or consent, and, as is now apparent, with insufficient oversight and accountability.

***Security Breaches Lead to Identity Theft***

60. According the U.S. Department of Justice Bureau of Justice Statistics, an estimated 17.6 million people were victims of one or more incidents of identity theft in 2014.<sup>2</sup>

61. The Federal Trade Commission ("FTC") cautions that identity theft wreaks havoc on consumers' finances, credit history and reputation and can take time, money, and patience to resolve.<sup>3</sup> Identity thieves use stolen personal

---

<sup>2</sup> See *Victims of Identity Theft, 2014*, DOJ, at 1 (2015), available at <https://www.bjs.gov/content/pub/pdf/vit14.pdf> (last visited Sept. 8, 2017).

<sup>3</sup> See *Taking Charge, What to Do If Your Identity is Stolen*, FTC, at 3 (2012), available at <http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf> (last visited Sept. 8, 2017).

information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.<sup>4</sup>

62. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the “cyber black-market” for a number of years.<sup>5</sup> As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen private information directly on various Internet websites, making the information publicly available.

63. In fact, “[a] quarter of consumers that received data breach letters [in 2012] wound up becoming a victim of identity fraud.”<sup>6</sup>

### ***The Monetary Value of Privacy Protections and Private Information***

64. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer’s personal information:

---

<sup>4</sup> The FTC defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.” 16 CFR § 603.2. The FTC describes “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including, among other things, “[n]ame, social security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number.” *Id.*

<sup>5</sup> Companies, in fact, also recognize Private Information as an extremely valuable commodity akin to a form of personal property. See John T. Soma et al., *Corporate Privacy Trend: The “Value” of Personally Identifiable Information (“PERSONAL INFORMATION”) Equals the “Value” of Financial Assets*, 15 RICH. J.L. & TECH. 11, at \*3–4 (2009).

<sup>6</sup> *One in Four that Receive Data Breach Letters Affected By Identity Theft*, available at <http://blog.kaspersky.com/data-breach-letters-affected-by-identity-theft/> (last visited Sept. 8, 2017).



The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.<sup>7</sup>

65. Commissioner Swindle's 2001 remarks are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a \$26 billion per year online advertising industry in the United States.<sup>8</sup> Indeed, as a nationwide consumer reporting agency, Equifax's entire line of business depends on the fact that the Private Information of consumers is valuable, both individually and in aggregate.

66. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In an FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point:

Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.<sup>9</sup>

---

<sup>7</sup> Federal Trade Commission Public Workshop, *The Information Marketplace: Merging and Exchanging Consumer Data*, available at [https://www.ftc.gov/sites/default/files/documents/public\\_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf](https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf) (last visited Sept. 8, 2017).

<sup>8</sup> See Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy*, The Wall Street Journal, <http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html> (last visited Sept. 8, 2017).

<sup>9</sup> *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, (Dec. 7, 2009),

67. Recognizing the high value that consumers place on their Private Information, many companies now offer consumers an opportunity to sell this information. The idea is to give consumers more power and control over the type of information that they share and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from their Private Information.<sup>10</sup> This business has created a new market for the sale and purchase of this valuable data.<sup>11</sup>

68. Consumers place a high value not only on their Private Information, but also on the privacy of that data. Researchers have already begun to shed light on how much consumers value their data privacy, and the amount is considerable. Indeed, studies confirm that the average direct financial loss for victims of identity theft in 2014 was \$1,349.”<sup>12</sup>

---

<http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf> (last visited Sept. 8, 2017).

<sup>10</sup> Steve Lohr, *You Want My Personal Data? Reward Me for It*, The New York Times, <http://www.nytimes.com/2010/07/18/business/18unboxed.html> (last visited Sept. 8, 2017).

<sup>11</sup> See *Web's Hot New Commodity: Privacy*, <http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html> (last visited Sept. 8, 2017).

<sup>12</sup> See Department of Justice, *Victims of Identity Theft, 2014*, at 6 (2015), <https://www.bjs.gov/content/pub/pdf/vit14.pdf> (last visited Sept. 8, 2017).

69. The value of Plaintiffs' and Class members' Private Information on the black market is substantial. By way of the Security Breach, Equifax has deprived Plaintiffs and Class members of the substantial value of their Private Information.

***Damages Sustained by Plaintiffs and the Other Class Members***

70. Plaintiffs and other members of the Class have suffered injury and damages, including, but not limited to: (i) an increased risk of identity theft and identity fraud; (ii) improper disclosure of their Private Information, which is now in the hands of criminals; (iii) the value of their time spent mitigating the increased risk of identity theft and identity fraud; (iv) deprivation of the value of their Private Information, for which there is a well-established national and international market—for which they are entitled to compensation.

71. Plaintiffs and the other Class members have suffered and will continue to suffer additional damages based on the opportunity cost and value of time that Plaintiffs and the other Class members have been forced to expend and must expend in the future to monitor their financial accounts and credit files as a result of the Security Breach.

72. Acknowledging the damage to Plaintiffs and Class members, Equifax is instructing consumers to “be vigilant in reviewing their account statements and credit reports,” “immediately report any unauthorized activity to their financial

institutions,” and to “monitor their personal information.” Plaintiffs and the other Class members now face a greater risk of identity theft.

## **V. CLASS ACTION ALLEGATIONS**

73. Plaintiffs bring Counts I–III, as set forth below, on behalf of themselves and as a class action, pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure, on behalf of a class defined as:

All persons whose Private Information was affected by the Security Breach that occurred from at least mid-May 2017 through July 2017, including all persons who Equifax’s “Check Potential Impact” tool identifies as being affected.

Excluded from the Class are Defendants and their affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

74. Plaintiffs bring Counts IV–XXXV set forth below on behalf of themselves and statewide classes for their respective states and those states with laws similar to their own defined as:

All persons in [Plaintiff’s state of citizenship] (and in those states with laws similar to the applicable law of [Plaintiff’s state of citizenship]) whose Private Information was affected by the Security Breach that occurred from at least mid-May 2017 through July 2017, including all persons who Equifax’s “Check Potential Impact” tool identifies as being affected.

Excluded from the Classes are Defendants and their affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

75. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

76. **Numerosity—Federal Rule of Civil Procedure 23(a)(1).** The members of the Class are so numerous that joinder of all Class members would be impracticable. On information and belief, Class members number over one hundred million. The precise number of Class members and their addresses are presently unknown to Plaintiffs, but may be ascertained from Equifax's books and records. Class members may be notified of the pendency of this action by mail, email, Internet postings, or publication.

77. **Commonality and Predominance—Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** Common questions of law and fact exist as to all Class members and predominate over questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

- a. Whether Equifax failed to use reasonable care and commercially reasonable methods to secure and safeguard Plaintiffs' and Class members' Private Information;
- b. Whether Equifax properly implemented its purported security measures to protect Plaintiffs' and Class members' Private Information from unauthorized capture, dissemination, and misuse;
- c. Whether Equifax took reasonable measures to determine the extent of the Security Breach after it first learned of same;
- d. Whether Equifax willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiffs' and Class members' Private Information;
- e. Whether Equifax was negligent in failing to properly secure and protect Plaintiffs' and Class members' Private Information;
- f. Whether TrustedID was negligent in failing to provide the promised TrustedID Premier service to consumers; and
- g. Whether Plaintiffs and the other members of the Class are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief.

78. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs, on behalf of themselves and other Class members. Similar or identical common law and statutory violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action.

79. **Typicality—Federal Rule of Civil Procedure 23(a)(3).** Plaintiffs' claims are typical of the claims of the other Class members because, among other things, all Class members were comparably injured through Defendants' uniform misconduct described above and were thus all subject to the Security Breach alleged herein. Further, there are no defenses available to Defendants that are unique to any Plaintiff.

80. **Adequacy of Representation—Federal Rule of Civil Procedure 23(a)(4).** Plaintiffs are adequate Class representatives because their interests do not conflict with the interests of the other Class members they seek to represent, they have retained counsel competent and experienced in complex class action litigation, and Plaintiffs will prosecute this action vigorously. The Class' interests will be fairly and adequately protected by Plaintiffs and their counsel.

81. **Superiority—Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiffs and the other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Equifax, so it would be impracticable for Class members to

individually seek redress for Equifax's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

## **CLAIMS**

### **COUNT I**

#### **Willful Failure to Comply with the Fair Credit Reporting Act, 15 U.S.C. § 1681n (Against Equifax Inc.)**

82. Plaintiffs incorporate paragraphs 1–81 as if fully set forth herein.

83. Equifax is a consumer reporting agency and is subject to the requirements of the federal Fair Credit Reporting Act ("FCRA").

84. Plaintiffs' and Class members' Private Information are consumer reports under FCRA, because the information bears on, among other things, their credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, physical/medical conditions, and mode of living, and is used or collected, in whole or in part, for the purpose of establishing Plaintiffs' and



the other Class members' eligibility for credit or insurance to be used primarily for personal, family, or household purposes.

85. FCRA enumerates the exclusive purposes for which a consumer reporting agency can furnish consumer reports. 15 U.S.C. § 1681b. FCRA also requires that:

Every consumer reporting agency shall maintain reasonable procedures designed to . . . limit the furnishing of consumer reports to the purposes listed under section 1681b of this title. These procedures shall require that prospective users of the information identify themselves, certify the purposes for which the information is sought, and certify that the information will be used for no other purpose.

15 U.S.C. § 1681e.

86. Equifax willfully, knowingly, or with reckless disregard, failed to adopt and maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes listed under 15 U.S.C. § 1681b when it enabled and facilitated the Security Breach. Equifax failed to address and eliminate known vulnerabilities in its systems that were curable and which were being actively attacked by hackers, failed to adequately vet users of its consumer reports, failed to inquire into suspicious circumstances despite possessing knowledge that put it on inquiry notice, and failed to reasonably monitor its customers' acquisition and use of consumer reports.

87. Equifax willfully, knowingly, or with reckless disregard, failed to comply with the FCRA's requirements with respect to Plaintiffs and the other Class members. As a result of Equifax's failures and in response to the commands of criminals, Equifax transmitted Plaintiffs' and other Class members' Private Information to criminals for illegitimate and unauthorized purposes.

88. As a further direct and foreseeable result of Equifax's willful noncompliance with FCRA, Plaintiffs' and the other Class members' Private Information will remain posted online in the public domain, compromised, and in possession of unauthorized third parties with fraudulent intent.

89. Plaintiffs and the other Class members seek any actual damages they have sustained, or in the alternative not less than \$100 and not more than \$1,000 in statutory damages; punitive damages as the court may allow, the costs of this action together with reasonable attorney's fees as determined by the court.

**COUNT II**  
**Negligent Failure to Comply with Fair Credit Reporting Act,**  
**15 U.S.C. § 1681o**  
**(Against Equifax Inc.)**

90. Plaintiffs incorporate paragraphs 1–81 as if fully set forth herein.

91. Equifax negligently failed to adopt and maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes listed under 15 U.S.C. § 1681b when it enabled and facilitated the Security Breach.

Equifax failed to address and eliminate known vulnerabilities in its systems that were curable and which were being actively attacked by hackers, failed to adequately vet users of its consumer reports, failed to inquire into suspicious circumstances despite possessing knowledge that put it on inquiry notice, and failed to reasonably monitor its customers' acquisition and use of consumer reports.

92. Plaintiffs' and the other Class members' Private Information was wrongfully furnished to criminals as a direct and foreseeable result of Equifax's negligent failure to adopt and maintain such reasonable procedures.

93. As a direct and foreseeable result, Plaintiffs' and the other Class members' consumer reports were accessed, made accessible to, stolen, furnished, and sold to unauthorized third parties for illegitimate and unauthorized purposes.

94. As a result of Equifax's negligent violations of FCRA, as described above, Plaintiffs and the other Class members were (and continue to be) injured and have suffered (and will continue to suffer) the damages described in detail above.

95. Plaintiffs and the other Class members, therefore, are entitled to compensation for their actual damages, as well as attorneys' fees, litigation expenses, and costs, pursuant to 15 U.S.C. § 1681o(a).

**COUNT III**  
**Negligence**  
**(Against All Defendants)**

96. Plaintiffs incorporate paragraphs 1–81 as if fully set forth herein.

97. Equifax owed numerous duties to Plaintiffs and the other members of the Class. These duties include the duty:

- a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;
- b. to protect Private Information in its possession using reasonable and adequate security procedures that are compliant with industry-standard practices; and
- c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches, including promptly notifying Plaintiff and the other members of the Class of the Security Breach.

98. Equifax knew or should have known the risks of collecting and storing Private Information and the importance of maintaining secure systems. Equifax knew of the many breaches that targeted other entities in the years preceding the Security Breach.

99. Given the nature of Equifax's business, the sensitivity and value of the information it aggregates, evaluates, and shares, and the resources at its disposal, Equifax should have identified the vulnerabilities to its systems and prevented the Security breach from occurring.

100. Equifax should have heeded the notifications by Cisco and US-CERT, among others, and illicit activity of hackers, and patched the vulnerabilities in its systems prior to the Security Breach in order to prevent the Security Breach from occurring.

101. Equifax knew or should have known that its systems did not adequately safeguard Plaintiffs' and the other Class members' Private Information.

102. Equifax breached the duties it owed to Plaintiffs and Class members in several ways, including:

- a. by failing to implement adequate security systems, protocols and practices sufficient to protect customer Private Information and thereby creating a foreseeable risk of harm;
- b. by failing to comply with the minimum industry data security standards;

- c. by failing to timely and accurately discovery and disclose to consumers that their Private Information had been improperly acquired or accessed; and
- d. by failing to provide the promised TrustedID Premier service.

103. But for Equifax's wrongful and negligent breach of the duties it owed to Plaintiffs and the other Class members, their Private Information would not have been compromised.

104. The injury and harm that Plaintiffs and the other Class members suffered was the direct and proximate result of Equifax's negligent conduct.

**COUNT IV**  
**Alaska Unfair Trade Practices and Consumer Protection Act**  
**Alaska Stat. § 45.50.471, et seq.**  
**(Against Equifax Inc.)**

105. Plaintiffs incorporate paragraphs 1–81 as if fully set forth herein.

106. Plaintiffs Russ and Jamie Benson and the other members of the Alaska Class were subjected to Equifax's unfair and deceptive acts or practices, in violation of AS § 45.50.471, in failing to properly implement adequate, commercially reasonable security measures to protect their Private Information and violating AS 45.48.010–45.48.090.

107. Equifax willfully ignored the clear and present risk of a security breach of its systems and failed to implement and maintain reasonable security measure to prevent, detect, and mitigate the Security Breach.

108. Equifax benefitted from not taking preventative measures and implementing adequate security measures that would have prevented, detected, and mitigated the Security Breach.

109. Equifax's failure to implement and maintain reasonable security measures caused and continues to cause substantial injury to the Bensons and the other Alaska Class members that is not offset by countervailing benefits to consumers or competition or reasonably avoidable by consumers.

110. Equifax's conduct offends public policy and is immoral, unethical, oppressive, and unscrupulous, and causes substantial injury to consumers.

111. The Bensons and the other Class members have suffered actual damages including improper disclosure of their Private Information, lost value of their Private Information, lost time and money incurred to mitigate and remediate the effects of the Security Breach, including the increased risk of identity theft that resulted and continues to face them.

112. Benson's and the other Class members' injuries were proximately caused by Equifax's violations of the Alaska Unfair Trade Practices and Consumer

Protection Act, which was conducted with reckless indifference toward the rights of others, such that an award of punitive damages is warranted.

**COUNT V**  
**Alaska Personal Information Protection Act,**  
**Alaska Stat. § 45.48.010, et seq.**  
**(Against Equifax Inc.)**

113. Plaintiffs incorporate paragraphs 1–81 as if fully set forth herein.

114. Equifax violated AS § 45.48010 by failing to notify the Bensons and all other Alaska residents of the Security Breach in the most expeditious time possible and without unreasonable delay. Equifax learned of the Security Breach as early as July 2017 but failed to notify affected persons until September 7, 2017.

115. Equifax knowingly violated Alaska Stat. § 45.48.430 by disclosing the Bensons’ and the other Class members’ social security numbers to third parties in the Security Breach.

116. The Bensons and the other Class members have suffered actual damages including improper disclosure of their Private Information, lost value of their Private Information, lost time and money incurred to mitigate and remediate the effects of the Security Breach and violation of PIPA, including the increased risk of identity theft that resulted and continues to face them.

117. The Bensons and the other Class members’ injuries were proximately caused by Equifax’s violations of the PIPA, which was conducted with reckless



indifference toward the rights of others, such that an award of punitive damages is warranted.

**COUNT VI**  
**District of Columbia Consumer Protection Procedures Act,**  
**D.C. Code § 28-3901, *et seq.***  
**(Against Equifax Inc.)**

118. Plaintiffs incorporate paragraphs 1–81 as if fully set forth herein.

119. Plaintiff Holly and the other members of the D.C. Class were subjected to Equifax’s unlawful trade practices, in violation of D.C. Code § 28-3904, in failing to properly implement adequate, commercially reasonable security measures to protect their Private Information.

120. Equifax willfully ignored the clear and present risk of a security breach of its systems and failed to implement and maintain reasonable security measure to prevent, detect, and mitigate the Security Breach.

121. Equifax benefitted from not taking preventative measures and implementing adequate security measures that would have prevented, detected, and mitigated the Security Breach.

122. Equifax’s failure to implement and maintain reasonable security measures caused and continues to cause substantial injury to Plaintiff Holly and the other D.C. Class members that is not offset by countervailing benefits to consumers or competition or reasonably avoidable by consumers.

123. Equifax's conduct offends public policy and is immoral, unethical, oppressive, and unscrupulous, and causes substantial injury to consumers.

124. Plaintiff Holly and the other Class members have suffered actual damages including improper disclosure of their Private Information, lost value of their Private Information, lost time and money incurred to mitigate and remediate the effects of the Security Breach, including the increased risk of identity theft that resulted and continues to face them.

125. Plaintiff Holly's and the other Class members' injuries were proximately caused by Equifax's violations of the D.C. Consumer Protection Procedures Act which was conducted with reckless indifference toward the rights of others, such that an award of punitive damages is warranted.

**COUNT VII**  
**District of Columbia Consumer Security Breach Notification Act,**  
**D.C. Code § 28-38511, et seq.**  
**(Against Equifax Inc.)**

126. Plaintiffs incorporate paragraphs 1–81 as if fully set forth herein.

127. Equifax violated D.C. Code § 28-3852 by failing to notify District of Columbia residents of the Security Breach in the most expedient time possible and without unreasonable delay. Equifax learned of the Security Breach as early as July 2017 but failed to notify affected persons until September 7, 2017.

128. Plaintiff Holly and the other Class members have suffered actual damages including improper disclosure of their Private Information, lost value of their Private Information, lost time and money incurred to mitigate and remediate the effects of the Security Breach and violation of D.C. Code § 28-3852, including the increased risk of identity theft that resulted and continues to face them.

129. Plaintiff Holly's and the other Class members' injuries were proximately caused by Equifax's violations of D.C. Code § 28-3852, which was conducted with reckless indifference toward the rights of others, such that an award of punitive damages is warranted.

**COUNT VIII**  
**Florida Deceptive and Unfair Trade Practices Act,**  
**Fla. Stat. § 501.204**  
**(Against Equifax Inc.)**

130. Plaintiffs incorporate paragraphs 1–81 as if fully set forth herein.

131. Plaintiffs Hinck, Green, and the other members of the Florida Class were subjected to Equifax's unconscionable and unfair and deceptive acts or practices, in violation of Fla. Stat. § 501.204, in failing to properly implement adequate, commercially reasonable security measures to protect their Private Information.

132. Equifax willfully ignored the clear and present risk of a security breach of its systems and failed to implement and maintain reasonable security measure to prevent, detect, and mitigate the Security Breach.

133. Equifax benefitted from not taking preventative measures and implementing adequate security measures that would have prevented, detected, and mitigated the Security Breach.

134. Equifax's failure to implement and maintain reasonable security measures caused and continues to cause substantial injury to Plaintiffs Hinck, Green, and the other Class members that is not offset by countervailing benefits to consumers or competition or reasonably avoidable by consumers.

135. Equifax's conduct offends public policy and is immoral, unethical, oppressive, and unscrupulous, and causes substantial injury to consumers.

136. Plaintiffs Hinck, Green, and the other Class members have suffered actual damages including improper disclosure of their Private Information, lost value of their Private Information, lost time and money incurred to mitigate and remediate the effects of the Security Breach, including the increased risk of identity theft that resulted and continues to face them.

137. Plaintiffs Hinck's, Green's, and the other Class members' injuries were proximately caused by Equifax's violations of the Florida Deceptive and Unfair Trade Practices Act.

**COUNT IX**  
**Illinois Consumer Fraud Act, 815 Ill. Comp. Stat. 505/2**  
**(Against Equifax Inc.)**

138. Plaintiffs incorporate paragraphs 1–81 as if fully set forth herein.

139. Plaintiff Chekmazov and the other members of the Class were subjected to Equifax's unfair or deceptive acts or practices, in violation of 815 Ill. Comp. Stat. 505/2, in failing to properly implement adequate, commercially reasonable security measures to protect their Private Information.

140. Equifax willfully ignored the clear and present risk of a security breach of its systems and failed to implement and maintain reasonable security measure to prevent, detect, and mitigate the Security Breach.

141. Equifax benefitted from not taking preventative measures and implementing adequate security measures that would have prevented, detected, and mitigated the Security Breach.

142. Equifax's failure to implement and maintain reasonable security measures caused and continues to cause substantial injury to Plaintiff Chekmazov

and the other Class members that is not offset by countervailing benefits to consumers or competition or reasonably avoidable by consumers.

143. Equifax's conduct offends public policy and is immoral, unethical, oppressive, and unscrupulous, and causes substantial injury to consumers.

144. Plaintiff Chekmazov and the other Class members have suffered actual damages including improper disclosure of their Private Information, lost value of their Private Information, lost time and money incurred to mitigate and remediate the effects of the Security Breach, including the increased risk of identity theft that resulted and continues to face them.

145. Plaintiff Chekmazov's and the other Class members' injuries were proximately caused by Equifax's violations of the Illinois Consumer Fraud Act, which was conducted with reckless indifference toward the rights of others, such that an award of punitive damages is warranted.

**COUNT X**  
**Illinois Personal Information Protection Act,**  
**815 Ill. Comp. Stat. 530/1, et seq.**  
**(Against Equifax Inc.)**

146. Plaintiffs incorporate paragraphs 1–81 as if fully set forth herein.

147. Equifax violated 815 Ill. Comp. Stat. 530/10(a) by failing to notify Illinois residents at no charge of the Security Breach in the most expedient time

possible and without unreasonable delay. Equifax learned of the Security Breach as early as July 2017 but failed to notify affected persons until September 7, 2017.

148. Equifax violated 815 Ill. Comp. Stat. 530/45 by failing to implement and maintain reasonable security measures to protect the Private Information from unauthorized access, acquisition, destruction, use, modification, or disclosure.

149. Plaintiff Chekmazov and the other Class members have suffered actual damages including improper disclosure of their Private Information, lost value of their Private Information, lost time and money incurred to mitigate and remediate the effects of the Security Breach and violation of PIPA, including the increased risk of identity theft that resulted and continues to face them.

150. Plaintiff Chekmazov's and the other Class members' injuries were proximately caused by Equifax's violations of the PIPA, which was conducted with reckless indifference toward the rights of others, such that an award of punitive damages is warranted.

**COUNT XI**  
**Kansas Fair Credit Reporting Act, Kan. Stat. § 50-701, et seq.**  
**(Against Equifax Inc.)**

151. Plaintiffs incorporate paragraphs 1–81 as if fully set forth herein.

152. Equifax is a consumer reporting agency and is subject to the requirements of the Kansas Fair Credit Reporting Act (“KFCRA”).

153. Plaintiff Iron Wing's and the other Class members' Private Information are consumer reports under KFCRA, because the information bears on, among other things, their credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, physical/medical conditions, and mode of living, and is used or collected, in whole or in part, for the purpose of establishing Plaintiff Iron Wing's and the other Class members' eligibility for credit or insurance to be used primarily for personal, family, or household purposes.

154. KFCRA enumerates the exclusive purposes for which a consumer reporting agency can furnish consumer reports. Kan. Stat. § 50-703. KFCRA also requires that:

Every consumer reporting agency shall maintain reasonable procedures designed to . . . limit the furnishing of consumer reports to the purposes listed under K.S.A. 50-703. These procedures shall require that prospective users of the information identify themselves, certify the purposes for which the information is sought, and certify that the information will be used for no other purpose.

Kan. Stat. § 50-706.

155. Equifax willfully, knowingly, with reckless disregard, or negligently failed to adopt and maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes listed under section fifty-one when it enabled and facilitated the Security Breach. Equifax failed to address and eliminate known



vulnerabilities in its systems that were curable and which were being actively attacked by hackers, failed to adequately vet users of its consumer reports, failed to inquire into suspicious circumstances despite possessing knowledge that put it on inquiry notice, and failed to reasonably monitor its customers' acquisition and use of consumer reports.

156. Equifax willfully, knowingly, with reckless disregard, or negligently failed to comply with the KFCRA's requirements with respect to Plaintiff Iron Wing and the other Class members. As a result of Equifax's failures, Equifax transmitted and furnished Plaintiff Iron Wing's and other Class members' Private Information to criminals for illegitimate and unauthorized purposes.

157. As a further direct and foreseeable result of Equifax's willful noncompliance with KFCRA, Plaintiff Iron Wing's and the other Class members' Private Information will remain posted online in the public domain, compromised, and in possession of unauthorized third parties with fraudulent intent.

**COUNT XII**  
**Kansas Consumer Protection Act, Kan. Stat. § 50-627**  
**(Against Equifax Inc.)**

158. Plaintiffs incorporate paragraphs 1–81 as if fully set forth herein.

159. Plaintiff Iron Wing and the other members of the Class were subjected to Equifax's unconscionable acts or practices, in violation of Kan. Stat. § 50-627,

in failing to properly implement adequate, commercially reasonable security measures to protect their Private Information.

160. Equifax willfully ignored the clear and present risk of a security breach of its systems and failed to implement and maintain reasonable security measure to prevent, detect, and mitigate the Security Breach.

161. Equifax benefitted from not taking preventative measures and implementing adequate security measures that would have prevented, detected, and mitigated the Security Breach.

162. Equifax's failure to implement and maintain reasonable security measures caused and continues to cause substantial injury to Plaintiff Iron Wing and the other Class members that is not offset by countervailing benefits to consumers or competition or reasonably avoidable by consumers.

163. Equifax's conduct offends public policy and is immoral, unethical, oppressive, and unscrupulous, and causes substantial injury to consumers.

164. Plaintiff Iron Wing and the other Class members have suffered actual damages including improper disclosure of their Private Information, lost value of their Private Information, lost time and money incurred to mitigate and remediate the effects of the Security Breach, including the increased risk of identity theft that resulted and continues to face them.

165. Plaintiff Iron Wing's and the other Class members' injuries were proximately caused by Equifax's violations of the Kansas Consumer Protection Act, which was conducted with reckless indifference toward the rights of others, such that an award of punitive damages is warranted.

**COUNT XIII**  
**Kentucky Consumer Protection Act, Ky. Rev. Stat. § 367.170**  
**(Against Equifax Inc.)**

166. Plaintiffs incorporate paragraphs 1–81 as if fully set forth herein.

167. Plaintiffs Koller and Oberst and the other members of the Class were subjected to Equifax's unfair acts or practices, in violation of Ky. Rev. Stat. § 367.170, in failing to properly implement adequate, commercially reasonable security measures to protect their Private Information.

168. Equifax willfully ignored the clear and present risk of a security breach of its systems and failed to implement and maintain reasonable security measure to prevent, detect, and mitigate the Security Breach.

169. Equifax benefitted from not taking preventative measures and implementing adequate security measures that would have prevented, detected, and mitigated the Security Breach.

170. Equifax's failure to implement and maintain reasonable security measures caused and continues to cause substantial injury to Plaintiffs Koller and

Oberst and the other Class members that is not offset by countervailing benefits to consumers or competition or reasonably avoidable by consumers.

171. Equifax's conduct offends public policy and is immoral, unethical, oppressive, and unscrupulous, and causes substantial injury to consumers.

172. Plaintiffs Koller and Oberst and the other Class members have suffered actual damages including improper disclosure of their Private Information, lost value of their Private Information, lost time and money incurred to mitigate and remediate the effects of the Security Breach, including the increased risk of identity theft that resulted and continues to face them.

173. Plaintiff Koller's and Oberst's and the other Class members' injuries were proximately caused by Equifax's violations of the Kentucky Consumer Protection Act, which was conducted with reckless indifference toward the rights of others, such that an award of punitive damages is warranted.

**COUNT XIV**  
**Maine Fair Credit Reporting Act, 10 M.R.S.A. § 1306, et seq.**  
**(Against Equifax Inc.)**

174. Plaintiffs incorporate paragraphs 1–81 as if fully set forth herein.

175. Equifax is a consumer reporting agency and is subject to the requirements of the Maine Fair Credit Reporting Act ("MFCRA").

176. Plaintiff Cooke and the other Class members' Private Information are consumer reports under MFCRA, because the information bears on, among other things, their credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, physical/medical conditions, and mode of living, and is used or collected, in whole or in part, for the purpose of establishing Plaintiff's and the other Class members' eligibility for credit or insurance to be used primarily for personal, family, or household purposes.

177. MFCRA provides that: "A person subject to this chapter shall comply with the federal Fair Credit Reporting Act and the provisions of 12 Code of Federal Regulations, Section 1022.1 et seq., as amended." 10 M.R.S.A. § 1309.

178. Equifax willfully, knowingly, with reckless disregard, or negligently failed to adopt and maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes listed under section fifty-one when it enabled and facilitated the Security Breach. Equifax failed to address and eliminate known vulnerabilities in its systems that were curable and which were being actively attacked by hackers, failed to adequately vet users of its consumer reports, failed to inquire into suspicious circumstances despite possessing knowledge that put it on inquiry notice, and failed to reasonably monitor its customers' acquisition and use of consumer reports.

179. Equifax willfully, knowingly, with reckless disregard, or negligently failed to comply with the MFCRA's requirements with respect to Plaintiff and the other Class members. As a result of Equifax's failures, Equifax transmitted and furnished Plaintiff's and other Class members' Private Information to criminals for illegitimate and unauthorized purposes.

180. As a further direct and foreseeable result of Equifax's willful, knowing, reckless, or negligent noncompliance with MFCRA, Plaintiff's and the other Class members' Private Information will remain posted online in the public domain, compromised, and in possession of unauthorized third parties with fraudulent intent.

**COUNT XV**  
**Maryland Consumer Protection Act, Md. Code § 13-101, et seq.**  
**(Against Equifax Inc.)**

181. Plaintiffs incorporate paragraphs 1–81 as if fully set forth herein.

182. Plaintiff Baumgardner and the other members of the Class were subjected to Equifax's unfair or deceptive trade practices, in violation of Md. Code § 13-301, in failing to properly implement adequate, commercially reasonable security measures to protect their Private Information.

183. Equifax willfully ignored the clear and present risk of a security breach of its systems and failed to implement and maintain reasonable security measure to prevent, detect, and mitigate the Security Breach.

184. Equifax benefitted from not taking preventative measures and implementing adequate security measures that would have prevented, detected, and mitigated the Security Breach.

185. Equifax's failure to implement and maintain reasonable security measures caused and continues to cause substantial injury to Plaintiff Baumgardner and the other Class members that is not offset by countervailing benefits to consumers or competition or reasonably avoidable by consumers.

186. Equifax's conduct offends public policy and is immoral, unethical, oppressive, and unscrupulous, and causes substantial injury to consumers.

187. Plaintiff Baumgardner and the other Class members have suffered actual damages including improper disclosure of their Private Information, lost value of their Private Information, lost time and money incurred to mitigate and remediate the effects of the Security Breach, including the increased risk of identity theft that resulted and continues to face them.

188. Plaintiff Baumgardner's and the other Class members' injuries were proximately caused by Equifax's violations of the Maryland Consumer Protection

Act, which was conducted with reckless indifference toward the rights of others, such that an award of punitive damages is warranted.

**COUNT XVI**  
**Maryland Personal Information Protection Act,**  
**Md. Code § 14-3501, et seq.**  
**(Against Equifax Inc.)**

189. Plaintiffs incorporate paragraphs 1–81 as if fully set forth herein.

190. Equifax violated Md. Code § 14-3504 by failing to notify Maryland residents of the Security Breach in a good faith and prompt manner as soon as reasonably practicable. Equifax learned of the Security Breach as early as July 2017 but failed to notify affected persons until September 7, 2017.

191. Equifax violated Md. Code § 14-3503 by failing to implement and maintain reasonable security procedures and practices that are appropriate, given the nature of the Private Information, from unauthorized access, use, modification, or disclosure.

192. Plaintiff Baumgardner and the other Class members have suffered actual damages including improper disclosure of their Private Information, lost value of their Private Information, lost time and money incurred to mitigate and remediate the effects of the Security Breach and violation of PIPA, including the increased risk of identity theft that resulted and continues to face them.



193. Plaintiff Baumgardner and the other Class members' injuries were proximately caused by Equifax's violations of the PIPA, which was conducted with reckless indifference toward the rights of others, such that an award of punitive damages is warranted.

**COUNT XVII**  
**Maryland Consumer Credit Reporting Agencies Act,**  
**Md. Code § 14-1201, et seq.**  
**(Against Equifax Inc.)**

194. Plaintiffs incorporate paragraphs 1–81 as if fully set forth herein.

195. Equifax is a consumer reporting agency and is subject to the requirements of the Maryland Consumer Credit Reporting Agencies Act (“MCCRAA”).

196. Plaintiff Baumgardner's and the other Class members' Private Information are consumer reports under MCCRAA, because the information bears on, among other things, their credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, physical/medical conditions, and mode of living, and is used or collected, in whole or in part, for the purpose of establishing Plaintiff Baumgardner's and the other Class members' eligibility for credit or insurance to be used primarily for personal, family, or household purposes.

197. MCCRAA enumerates the exclusive purposes for which a consumer reporting agency can furnish consumer reports. Md. Code § 14-1202. MCCRAA also requires that:

(1) A consumer reporting agency shall maintain reasonable procedures designed to . . . limit the furnishing of consumer reports to the purposes listed under § 14-1202.

(2) The procedures at a minimum shall require that prospective users of the information identify themselves, certify the purposes for which the information is sought, and certify that the information will be used for no other purpose.

(3) A consumer reporting agency shall make a reasonable effort to verify the identity of a new prospective user and the uses certified by the prospective user prior to furnishing the user a consumer report.

Md. Code § 14-1205.

198. Equifax willfully, knowingly, with reckless disregard, or negligently failed to adopt and maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes listed under section fifty-one when it enabled and facilitated the Security Breach. Equifax failed to address and eliminate known vulnerabilities in its systems that were curable and which were being actively attacked by hackers, failed to adequately vet users of its consumer reports, failed to inquire into suspicious circumstances despite possessing knowledge that put it on inquiry notice, and failed to reasonably monitor its customers' acquisition and use of consumer reports.

199. Equifax willfully, knowingly, with reckless disregard, or negligently failed to comply with the MCCRAA's requirements with respect to Plaintiff Baumgardner and the other Class members. As a result of Equifax's failures, Equifax transmitted and furnished Plaintiff Baumgardner and other Class members' Private Information to criminals for illegitimate and unauthorized purposes.

200. As a further direct and foreseeable result of Equifax's willful noncompliance with MCCRAA, Plaintiff Baumgardner and the other Class members' Private Information will remain posted online in the public domain, compromised, and in possession of unauthorized third parties with fraudulent intent.

**COUNT XVIII**  
**Maryland Social Security Number Privacy Act, Md. Code § 14-3401, et seq.**  
**(Against Equifax Inc.)**

201. Plaintiffs incorporate paragraphs 1–81 as if fully set forth herein.

202. Equifax violated Md. Code § 14-3402 by publicly posting or displaying Plaintiff Baumgardner's and the other Class members' social security numbers; printing an individual's social security number on a card required for the individual to access products or services provided by the person; requiring Plaintiff and the other Class members to transmit their social security numbers over the

Internet in an unsecure and unencrypted manner; or requiring Plaintiff and the other Class members to use their social security number to access an Internet Web site while failing to implement sufficient security.

203. Equifax willfully, knowingly, with reckless disregard, or negligently failed to comply with the Md. Code § 14-34702 with respect to Plaintiff Baumgardner and the other Class members. As a result of Equifax's failures, Equifax transmitted and furnished Plaintiff Baumgardner and other Class members' Private Information to criminals for illegitimate and unauthorized purposes.

204. As a further direct and foreseeable result of Equifax's willful noncompliance with Md. Code § 14-3402, Plaintiff Baumgardner and the other Class members' Private Information will remain posted online in the public domain, compromised, and in possession of unauthorized third parties with fraudulent intent.

**COUNT XIX**  
**Massachusetts Fair Credit Reporting Act,**  
**Mass. Gen. Laws ch. 93, § 50, et seq.**  
**(Against Equifax Inc.)**

205. Plaintiffs incorporate paragraphs 1–81 as if fully set forth herein.

206. Equifax is a consumer reporting agency and is subject to the requirements of the Massachusetts Fair Credit Reporting Act ("MFCRA").

207. Plaintiff Poligian's and the other Class members' Private Information are consumer reports under MFCRA, because the information bears on, among other things, their credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, physical/medical conditions, and mode of living, and is used or collected, in whole or in part, for the purpose of establishing Plaintiffs' and the other Class members' eligibility for credit or insurance to be used primarily for personal, family, or household purposes.

208. MFCRA enumerates the exclusive purposes for which a consumer reporting agency can furnish consumer reports. Mass. Gen. Law ch. 93, § 51.

MFCRA also requires that:

Every consumer reporting agency shall maintain reasonable procedures designed to . . . limit the furnishing of consumer reports to the purposes listed under section fifty-one. These procedures shall require that prospective users of the information identify themselves, certify the purposes for which the information is sought, and certify that the information will be used for no other purpose.

Mass. Gen. Law ch. 93, § 54.

209. Equifax willfully, knowingly, with reckless disregard, or negligently failed to adopt and maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes listed under section fifty-one when it enabled and facilitated the Security Breach. Equifax failed to address and eliminate known vulnerabilities in its systems that were curable and which were being actively

attacked by hackers, failed to adequately vet users of its consumer reports, failed to inquire into suspicious circumstances despite possessing knowledge that put it on inquiry notice, and failed to reasonably monitor its customers' acquisition and use of consumer reports.

210. Equifax willfully, knowingly, with reckless disregard, or negligently failed to comply with the FCRA's requirements with respect to Plaintiff Poligian and the other Class members. As a result of Equifax's failures, Equifax transmitted and furnished Plaintiff Poligian's and other Class members' Private Information to criminals for illegitimate and unauthorized purposes.

211. As a further direct and foreseeable result of Equifax's willful noncompliance with MFCRA, Plaintiff Poligian's and the other Class members' Private Information will remain posted online in the public domain, compromised, and in possession of unauthorized third parties with fraudulent intent.

**COUNT XX**  
**Massachusetts Consumer Protection Act, Mass. Gen. Laws ch. 93A, § 2**  
**(Against Equifax Inc.)**

212. Plaintiffs incorporate paragraphs 1–81 as if fully set forth herein.

213. Plaintiff Poligian and the other members of the Class were subjected to Equifax's unfair or deceptive acts or practices, in violation of Mass. Gen. Laws

ch. 93, § 2, in failing to properly implement adequate, commercially reasonable security measures to protect their Private Information.

214. Equifax willfully ignored the clear and present risk of a security breach of its systems and failed to implement and maintain reasonable security measure to prevent, detect, and mitigate the Security Breach.

215. Equifax benefitted from not taking preventative measures and implementing adequate security measures that would have prevented, detected, and mitigated the Security Breach.

216. Equifax's failure to implement and maintain reasonable security measures caused and continues to cause substantial injury to Plaintiff Poligian and the other Class members that is not offset by countervailing benefits to consumers or competition or reasonably avoidable by consumers.

217. Equifax's conduct offends public policy and is immoral, unethical, oppressive, and unscrupulous, and causes substantial injury to consumers.

218. Plaintiff Poligian and the other Class members have suffered actual damages including improper disclosure of their Private Information, lost value of their Private Information, lost time and money incurred to mitigate and remediate the effects of the Security Breach, including the increased risk of identity theft that resulted and continues to face them.

219. Plaintiff Poligian's and the other Class members' injuries were proximately caused by Equifax's violations of the Mass. Gen. Laws ch. 93A, § 2, which was conducted with reckless indifference toward the rights of others, such that an award of punitive damages is warranted.

**COUNT XXI**  
**New Hampshire Fair Credit Reporting Act, N.H. Rev. Stat. § 359-B:1, et seq.**  
**(Against Equifax Inc.)**

220. Plaintiffs incorporate paragraphs 1–81 as if fully set forth herein.

221. Equifax is a consumer reporting agency and is subject to the requirements of the New Hampshire Fair Credit Reporting Act (“NHFCRA”).

222. Plaintiffs McCable's and Andreica's and the other Class members' Private Information are consumer reports under NHFCRA, because the information bears on, among other things, their credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, physical/medical conditions, and mode of living, and is used or collected, in whole or in part, for the purpose of establishing Plaintiffs' and the other Class members' eligibility for credit or insurance to be used primarily for personal, family, or household purposes.



223. NHFCRA enumerates the exclusive purposes for which a consumer reporting agency can furnish consumer reports. N.H. Rev. Stat. § 359-B:4. NHFCRA also requires that:

Every consumer reporting agency shall maintain reasonable procedures designed to . . . limit the furnishing of consumer reports to the purposes listed under RSA 359-B:4. These procedures shall require that prospective users of the information identify themselves, certify the purposes for which the information is sought, and certify that the information will be used for no other purpose.

N.H. Rev. Stat. § 359-B:7.

224. Equifax willfully, knowingly, with reckless disregard, or negligently failed to adopt and maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes listed under section fifty-one when it enabled and facilitated the Security Breach. Equifax failed to address and eliminate known vulnerabilities in its systems that were curable and which were being actively attacked by hackers, failed to adequately vet users of its consumer reports, failed to inquire into suspicious circumstances despite possessing knowledge that put it on inquiry notice, and failed to reasonably monitor its customers' acquisition and use of consumer reports.

225. Equifax willfully, knowingly, with reckless disregard, or negligently failed to comply with the FCRA's requirements with respect to Plaintiffs and the other Class members. As a result of Equifax's failures, Equifax transmitted and

furnished Plaintiffs' and other Class members' Private Information to criminals for illegitimate and unauthorized purposes.

226. As a further direct and foreseeable result of Equifax's willful, knowing, reckless, or negligent noncompliance with NHFCRA, Plaintiffs' and the other Class members' Private Information will remain posted online in the public domain, compromised, and in possession of unauthorized third parties with fraudulent intent.

**COUNT XXII**  
**New Hampshire Consumer Protection Act, N.H. Gen. Stat. § 358-A:2, et seq.**  
**(Against Equifax Inc.)**

227. Plaintiffs incorporate paragraphs 1–81 as if fully set forth herein.

228. Plaintiffs McCable and Andreica and the other members of the Class were subjected to Equifax's unfair or deceptive acts or practices, in violation of N.H. Gen. Stat. § 358-A:2, in failing to properly implement adequate, commercially reasonable security measures to protect their Private Information.

229. Equifax willfully ignored the clear and present risk of a security breach of its systems and failed to implement and maintain reasonable security measure to prevent, detect, and mitigate the Security Breach.

230. Equifax benefitted from not taking preventative measures and implementing adequate security measures that would have prevented, detected, and mitigated the Security Breach.

231. Equifax's failure to implement and maintain reasonable security measures caused and continues to cause substantial injury to Plaintiffs and the other Class members that is not offset by countervailing benefits to consumers or competition or reasonably avoidable by consumers.

232. Equifax's conduct offends public policy and is immoral, unethical, oppressive, and unscrupulous, and causes substantial injury to consumers.

233. Plaintiffs and the other members have suffered actual damages including improper disclosure of their Private Information, lost value of their Private Information, lost time and money incurred to mitigate and remediate the effects of the Security Breach, including the increased risk of identity theft that resulted and continues to face them.

234. Plaintiffs' and the other Class members' injuries were proximately caused by Equifax's violations of N.H. Gen. Stat. § 358-A:2, which was conducted with reckless indifference toward the rights of others, such that an award of punitive damages is warranted.

**COUNT XXIII**  
**New Hampshire Notice of Security Breach Act**

**N.H. Rev. Stat. § 359-C:19, et seq.**  
**(Against Equifax Inc.)**

235. Plaintiffs incorporate paragraphs 1–81 as if fully set forth herein.

236. Equifax violated N.H. Rev. Stat. § 359-C: 20 by failing to notify New Hampshire residents of the Security Breach as soon as possible. Equifax learned of the Security Breach as early as July 2017 but failed to notify affected persons until September 7, 2017.

237. Plaintiffs McCable and Andreica and the other Class members have suffered actual damages including improper disclosure of their Private Information, lost value of their Private Information, lost time and money incurred to mitigate and remediate the effects of the Security Breach and violation of PIPA, including the increased risk of identity theft that resulted and continues to face them.

238. Plaintiffs’ and the other Class members’ injuries were proximately caused by Equifax’s violations of N.H. Rev. Stat. § 359-C: 20, which was conducted with reckless indifference toward the rights of others, such that an award of punitive damages is warranted.

**COUNT XXIV**  
**North Carolina Unfair and Deceptive Trade Practices Act,**  
**N.C. Gen. Stat. Ann. § 75-1, et seq.**  
**(Against Equifax Inc.)**

239. Plaintiffs incorporate paragraphs 1–81 as if fully set forth herein.

240. Plaintiff Brown and the other members of the Class were subjected to Equifax’s unfair or deceptive acts or practices, in violation of N.C. Gen. Stat. Ann §75-1 in failing to properly implement adequate, commercially reasonable security measures to protect their Private Information.

241. Equifax willfully ignored the clear and present risk of a security breach of its systems and failed to implement and maintain reasonable security measure to prevent, detect, and mitigate the Security Breach.

242. Equifax benefitted from not taking preventative measures and implementing adequate security measures that would have prevented, detected, and mitigated the Security Breach.

243. Equifax’s failure to implement and maintain reasonable security measures caused and continues to cause substantial injury to Plaintiff Brown and the other Class members that is not offset by countervailing benefits to consumers or competition or reasonable avoidable by consumers.

244. Equifax’s conduct offends public policy and is immoral, unethical, oppressive, and unscrupulous, and causes substantial injury to consumers.

245. Plaintiff Brown and the other Class members have suffered actual damages including improper disclosure of their Private Information, lost value of

their Private Information, lost time and money incurred to mitigate and remediate the effects of the Security Breach, including the increased risk of identity theft that resulted and continues to face them.

246. Plaintiff Brown's and the other Class members' injuries were proximately caused by Equifax's violations of the North Carolina Unfair Deceptive Trade Practices Act, which was conducted with reckless indifference toward the rights of others, such that an award of punitive damages is warranted.

**COUNT XXV**  
**North Carolina Protection from Security Breaches Act,**  
**N.C. Gen. Stat. § 75-65**  
**(Against Equifax Inc.)**

247. Plaintiffs incorporate paragraphs 1–81 as if fully set forth herein.

248. Equifax violated N.C. Gen. Stat. § 75-65 by failing to notify North Carolina residents of the Security Breach without unreasonable delay. Equifax learned of the Security Breach as early as July 2017 but failed to notify affected persons until September 7, 2017.

249. Plaintiff Brown and the other Class members have suffered actual damages including improper disclosure of their Private Information, lost value of their Private Information, lost time and money incurred to mitigate and remediate the effects of the Security Breach and violation of N.C. Gen. Stat. § 75-65,

including the increased risk of identity theft that resulted and continues to face them.

250. Plaintiff Brown's and the other Class members' injuries were proximately caused by Equifax's violations of N.C. Gen. Stat. § 75-65, which was conducted with reckless indifference toward the rights of others, such that an award of punitive damages is warranted.

**COUNT XXVI**  
**New Mexico Unfair Practices Act, N.M. Stat. § 57-12-1, et seq.**  
**(Against Equifax Inc.)**

251. Plaintiffs incorporate paragraphs 1–81 as if fully set forth herein.

252. Plaintiff Szekely and the other members of the Class were subjected to Equifax's unfair or deceptive trade practices and unconscionable trade practices, in violation of N.M. Stat. § 57-12-1 in failing to properly implement adequate, commercially reasonable security measures to protect their Private Information.

253. Equifax willfully ignored the clear and present risk of a security breach of its systems and failed to implement and maintain reasonable security measure to prevent, detect, and mitigate the Security Breach.

254. Equifax benefitted from not taking preventative measures and implementing adequate security measures that would have prevented, detected, and mitigated the Security Breach.

255. Equifax's failure to implement and maintain reasonable security measures caused and continues to cause substantial injury to Plaintiff Szekely and the other Class members that is not offset by countervailing benefits to consumers or competition or reasonable avoidable by consumers.

256. Equifax's conduct offends public policy and is immoral, unethical, oppressive, and unscrupulous, and causes substantial injury to consumers.

257. Plaintiff Szekely and the other Class members have suffered actual damages including improper disclosure of their Private Information, lost value of their Private Information, lost time and money incurred to mitigate and remediate the effects of the Security Breach, including the increased risk of identity theft that resulted and continues to face them.

258. Plaintiff Szekely's and the other Class members' injuries were proximately caused by Equifax's violations of the New Mexico Unfair Practices Act, which was conducted with reckless indifference toward the rights of others, such that an award of treble damages, statutory damages, and punitive damages is warranted.

**COUNT XXVII**  
**New Mexico Privacy Protection Act, N.M. Stat. § 57-12B-1, et seq.**  
**(Against Equifax Inc.)**

259. Plaintiffs incorporate paragraphs 1–81 as if fully set forth herein.



260. Equifax violated N.M. Stat. §§ 57-12B-3, 4 by failing to properly implement adequate, commercially reasonable security measures to protect their Private Information.

261. Equifax willfully ignored the clear and present risk of a security breach of its systems and failed to implement and maintain reasonable security measure to prevent, detect, and mitigate the Security Breach.

262. Plaintiff Szekely and the other Class members have suffered actual damages including improper disclosure of their Private Information, lost value of their Private Information, lost time and money incurred to mitigate and remediate the effects of the Security Breach, including the increased risk of identity theft that resulted and continues to face them.

263. Plaintiff Szekely's and the other Class members' injuries were proximately caused by Equifax's violations of the New Mexico Privacy Protection Act, which was conducted with reckless indifference toward the rights of others, such that an award of treble damages, statutory damages, and punitive damages is warranted.

**COUNT XXVIII**  
**Ohio Consumer Sales Practices Act, Ohio Rev. Code § 1345, et seq.**  
**(Against Equifax Inc.)**

264. Plaintiffs incorporate paragraphs 1–81 as if fully set forth herein.

265. Plaintiffs Kellie and Michael Jay Williams and the other members of the Class were subjected to Equifax's unfair or deceptive acts or practices and unconscionable trade practices, in violation of Ohio Rev. Code § 1345.02 in failing to properly implement adequate, commercially reasonable security measures to protect their Private Information.

266. Equifax willfully ignored the clear and present risk of a security breach of its systems and failed to implement and maintain reasonable security measure to prevent, detect, and mitigate the Security Breach.

267. Equifax benefitted from not taking preventative measures and implementing adequate security measures that would have prevented, detected, and mitigated the Security Breach.

268. Equifax's failure to implement and maintain reasonable security measures caused and continues to cause substantial injury to the Williams and the other Class members that is not offset by countervailing benefits to consumers or competition or reasonable avoidable by consumers.

269. Equifax's conduct offends public policy and is immoral, unethical, oppressive, and unscrupulous, and causes substantial injury to consumers.

270. The Williams and the other Class members have suffered actual damages including improper disclosure of their Private Information, lost value of

their Private Information, lost time and money incurred to mitigate and remediate the effects of the Security Breach, including the increased risk of identity theft that resulted and continues to face them.

271. The Williams' and the other Class members' injuries were proximately caused by Equifax's violations of the Ohio Consumer Sales Practices Act, which was conducted with reckless indifference toward the rights of others, such that an award of treble damages, statutory damages, and punitive damages is warranted.

**COUNT XXIX**  
**Oregon Unfair Trade Practices Act, Or. Rev. Stat. § 646.605, et seq.**  
**(Against Equifax Inc.)**

272. Plaintiffs incorporate paragraphs 1–81 as if fully set forth herein.

273. Plaintiffs Corree and Chad Roofener and the other members of the Class were subjected to Equifax's unfair and deceptive conduct, in violation of Or. Rev. Stat. § 646.608 in failing to properly implement adequate, commercially reasonable security measures to protect their Private Information.

274. Equifax willfully ignored the clear and present risk of a security breach of its systems and failed to implement and maintain reasonable security measure to prevent, detect, and mitigate the Security Breach.

275. Equifax benefitted from not taking preventative measures and implementing adequate security measures that would have prevented, detected, and mitigated the Security Breach.

276. Equifax's failure to implement and maintain reasonable security measures caused and continues to cause substantial injury to the Roofeners and the other Class members that is not offset by countervailing benefits to consumers or competition or reasonable avoidable by consumers.

277. Equifax's conduct offends public policy and is immoral, unethical, oppressive, and unscrupulous, and causes substantial injury to consumers.

278. The Roofeners and the other Class members have suffered actual damages including improper disclosure of their Private Information, lost value of their Private Information, lost time and money incurred to mitigate and remediate the effects of the Security Breach, including the increased risk of identity theft that resulted and continues to face them.

279. The Roofeners and the other Class members' injuries were proximately caused by Equifax's violations of the Oregon Unfair Trade Practices Act, which was conducted with reckless indifference toward the rights of others, such that an award of punitive damages is warranted.

**COUNT XXX**  
**Oregon Consumer Identity Theft Protection Act,**

**Or. Rev. Stat. § 646A.600, et seq.**  
**(Against Equifax Inc.)**

280. Plaintiffs incorporate paragraphs 1–81 as if fully set forth herein.

281. Equifax violated Or. Rev. Stat. § 646A.604 by failing to notify Oregon residents of the Security Breach in the most expeditious manner possible. Equifax learned of the Security Breach as early as July 2017 but failed to notify affected persons until September 7, 2017.

282. Equifax violated Or. Rev. Stat. § 646A.620 by publicly posting or publicly displaying the Roofeners’ and the other Class members’ social security numbers and otherwise making their social security numbers available to the public.

283. Equifax violated Or. Rev. Stat. § 646A.622 by failing to develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the Roofeners’ and the other Class members’ Private Information.

284. The Roofeners and the other Class members have suffered actual damages including improper disclosure of their Private Information, lost value of their Private Information, lost time and money incurred to mitigate and remediate the effects of the Security Breach and violations of the Oregon Consumer Identity

Theft Protection Act, including the increased risk of identity theft that resulted and continues to face them.

285. The Roofeners and the other Class members' injuries were proximately caused by Equifax's violations of the Oregon Consumer Identity Theft Protection Act, which were conducted with reckless indifference toward the rights of others, such that an award of punitive damages is warranted.

**COUNT XXXI**  
**Texas Deceptive Trade Practices-Consumer Protection Act,**  
**Tex. Bus. & Com. Code § 17.41, et seq.**  
**(Against Equifax Inc.)**

286. Plaintiffs incorporate paragraphs 1–81 as if fully set forth herein.

287. Plaintiff Jaetzold and the other members of the Class were subjected to Equifax's unconscionable actions, in violation of Tex. Bus. & Com. Code § 17.41, *et seq.*, and Tex. Bus. & Com. Code § 521.051–521.053, in failing to properly implement adequate, commercially reasonable security measures to protect their Private Information.

288. Equifax willfully ignored the clear and present risk of a security breach of its systems and failed to implement and maintain reasonable security measure to prevent, detect, and mitigate the Security Breach.

289. Equifax benefitted from not taking preventative measures and implementing adequate security measures that would have prevented, detected, and mitigated the Security Breach.

290. Equifax's failure to implement and maintain reasonable security measures caused and continues to cause substantial injury to Plaintiff Jaetzold and the other Class members that is not offset by countervailing benefits to consumers or competition or reasonable avoidable by consumers.

291. Equifax's conduct offends public policy and is immoral, unethical, oppressive, and unscrupulous, and causes substantial injury to consumers.

292. Plaintiff Jaetzold and the other Class members have suffered actual damages including improper disclosure of their Private Information, lost value of their Private Information, lost time and money incurred to mitigate and remediate the effects of the Security Breach, including the increased risk of identity theft that resulted and continues to face them.

293. Plaintiff Jaetzold's and the other Class members' injuries were proximately caused by Equifax's violations of the Texas Deceptive Trade Practices-Consumer Protection Act, which was conducted with reckless indifference toward the rights of others, such that an award of punitive damages is warranted.

**COUNT XXXII**  
**Virginia Breach of Personal Information Notification Statute,**  
**Va. Code § 18.2-186.6**  
**(Against Equifax Inc.)**

294. Plaintiffs incorporate paragraphs 1–81 as if fully set forth herein.

295. Equifax violated Va. Code § 18.2-186.6 by failing to notify Virginia residents of the Security Breach without unreasonable delay. Equifax learned of the Security Breach as early as July 2017 but failed to notify affected persons until September 7, 2017.

296. Plaintiff Erickson and the other Class members have suffered actual damages including improper disclosure of their Private Information, lost value of their Private Information, lost time and money incurred to mitigate and remediate the effects of the Security Breach and violation of Va. Code § 18.2-186.6, including the increased risk of identity theft that resulted and continues to face them.

297. Plaintiff Erickson's and the other Class members' injuries were proximately caused by Equifax's violations of Va. Code § 18.2-186.6, which was conducted with reckless indifference toward the rights of others, such that an award of punitive damages is warranted.

**COUNT XXXIII**  
**Washington Fair Credit Reporting Act, Wash. Rev. Code § 19.182.005, et seq.**  
**(Against Equifax Inc.)**



298. Plaintiffs incorporate paragraphs 1–81 as if fully set forth herein.

299. Equifax is a consumer reporting agency and is subject to the requirements of the Washington Fair Credit Reporting Act (“WFCRA”).

300. Plaintiff Peacock’s and Class members’ Private Information are consumer reports under WFCRA, because the information bears on, among other things, their credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, physical/medical conditions, and mode of living, and is used or collected, in whole or in part, for the purpose of establishing Peacock’s and the other Class members’ eligibility for credit or insurance to be used primarily for personal, family, or household purposes.

301. WFCRA enumerates the exclusive purposes for which a consumer reporting agency can furnish consumer reports. Wash. Rev. Code § 19.182.020. WFCRA also requires that:

A consumer reporting agency shall maintain reasonable procedures designed to . . . limit the furnishing of consumer reports to the purposes listed under RCW 19.182.020. These procedures shall require that prospective users of the information identify themselves, certify the purposes for which the information is sought, and certify that the information will be used for no other purpose.

Wash. Rev. Code § 19.182.060.

302. Equifax willfully, knowingly, or with reckless disregard, failed to adopt and maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes listed under Wash. Rev. Code § 19.182.020 when it enabled and facilitated the Security Breach. Equifax failed to address and eliminate known vulnerabilities in its systems that were curable and which were being actively attacked by hackers, failed to adequately vet users of its consumer reports, failed to inquire into suspicious circumstances despite possessing knowledge that put it on inquiry notice, and failed to reasonably monitor its customers' acquisition and use of consumer reports.

303. Equifax willfully, knowingly, or with reckless disregard, failed to comply with the WFCRA's requirements with respect to Plaintiff Peacock and the other Class members. As a result of Equifax's failures, Equifax transmitted and furnished Plaintiff Peacock's and other Class members' Private Information to criminals for illegitimate and unauthorized purposes.

304. As a further direct and foreseeable result of Equifax's willful noncompliance with WFCRA, Plaintiff Peacock's and the other Class members' Private Information will remain posted online in the public domain, compromised, and in possession of unauthorized third parties with fraudulent intent.

305. Plaintiff Peacock's and the other Class members' injuries were proximately caused by Equifax's violations of the Washington Fair Credit Reporting Act, which was conducted with willful and reckless indifference toward the rights of others, such that an award of treble damages, statutory damages, and punitive damages is warranted.

**COUNT XXXIV**  
**Washington Consumer Protection Act, Wash. Rev. Code § 19.86.020, et seq.**  
**(Against Equifax Inc.)**

306. Plaintiffs incorporate paragraphs 1–81 as if fully set forth herein.

307. Plaintiff Peacock and the other members of the Class were subjected to Equifax's unfair or deceptive trade practices, in violation of Wash. Rev. Code § 19.86.020 in failing to properly implement adequate, commercially reasonable security measures to protect their Private Information.

308. Equifax willfully ignored the clear and present risk of a security breach of its systems and failed to implement and maintain reasonable security measure to prevent, detect, and mitigate the Security Breach.

309. Equifax benefitted from not taking preventative measures and implementing adequate security measures that would have prevented, detected, and mitigated the Security Breach.

310. Equifax's failure to implement and maintain reasonable security measures caused and continues to cause substantial injury to Plaintiff Peacock and the other Class members that is not offset by countervailing benefits to consumers or competition or reasonable avoidable by consumers.

311. Equifax's conduct offends public policy and is immoral, unethical, oppressive, and unscrupulous, and causes substantial injury to consumers.

312. Plaintiff Peacock and the other Class members have suffered actual damages including improper disclosure of their Private Information, lost value of their Private Information, lost time and money incurred to mitigate and remediate the effects of the Security Breach, including the increased risk of identity theft that resulted and continues to face them.

313. Plaintiff Peacock's and the other Class members' injuries were proximately caused by Equifax's violations of the Washington Consumer Protection Act, which was conducted with reckless indifference toward the rights of others, such that an award of treble damages, statutory damages, and punitive damages is warranted.

**COUNT XXXV**  
**Washington Data Breach Notification Statute,**  
**Wash. Rev. Code § 19.255.010, et seq.**  
**(Against Equifax Inc.)**

314. Plaintiffs incorporate paragraphs 1–81 as if fully set forth herein.

315. Equifax violated Wash. Rev. Code § 19.255.010 by failing to notify Washington residents of the Security Breach following its discovery. Equifax learned of the Security Breach as early as July 2017 but failed to notify affected persons until September 7, 2017.

316. Plaintiff Peacock and the other Class members have suffered actual damages including improper disclosure of their Private Information, lost value of their Private Information, lost time and money incurred to mitigate and remediate the effects of the Security Breach and violation of Wash. Rev. Code § 19.255.010, including the increased risk of identity theft that resulted and continues to face them.

317. Plaintiff Peacock's and the other Class members' injuries were proximately caused by Equifax's violations of Wash. Rev. Code § 19.255.010, which was conducted with reckless indifference toward the rights of others, such that an award of punitive damages is warranted.

### **DEMAND FOR JURY TRIAL**

Plaintiffs demand a trial by jury of all claims in this complaint so triable.

### **REQUEST FOR RELIEF**

WHEREFORE, Plaintiffs, individually and on behalf of the other members of the Classes proposed in this Complaint, respectfully requests that the Court enter judgment in their favor and against Defendants, as follows:

- A. Certifying the Classes as requested herein, designating Plaintiffs as Class Representatives, and appointing Ben Barnow of Barnow and Associates, P.C. as Class Counsel;
- B. Ordering Defendants to pay actual damages to Plaintiffs and the other members of the Classes;
- C. Ordering Defendants to pay statutory damages to Plaintiffs and the other members of the Classes;
- D. Ordering Defendants to pay punitive damages, as allowable by law, to Plaintiffs and the other members of the Classes;
- E. Ordering Defendants to pay attorneys' fees and litigation costs to Plaintiffs;
- F. Ordering Defendants to pay both pre- and post-judgment interest on any amounts awarded as allowable by law; and
- G. Ordering such other and further relief as may be just and proper.

Date: September 25, 2017

Respectfully submitted,

/s/ David J. Worley

David J. Worley

GA Bar No. 776665

James M. Evangelista

GA Bar No. 707807

Kristi Stahnke McGregor

Georgia Bar No. 674012

**EVANGELISTA WORLEY, LLC**

8100A Roswell Road  
Suite 100  
Atlanta, GA 30350  
Tel: (404) 205-8400  
david@ewlawllc.com  
jim@ewlawllc.com  
kristi@ewlawllc.com

Ben Barnow

IL Bar No. 0118265  
(*Pro hac vice* to be filed)

Erich P. Schork

IL Bar No. 6291153  
(*Pro hac vice* to be filed)

**BARNOW AND ASSOCIATES, P.C.**

One North LaSalle Street, Suite 4600  
Chicago, IL 60602  
Tel: (312) 621-2000  
Fax: (312) 641-5504  
b.barnow@barnowlaw.com  
e.schork@barnowlaw.com

Timothy G. Blood

CA Bar No. 149343  
(*Pro hac vice* to be filed)

**BLOOD HURST & O'REARDON, LLP**

701 B Street, Suite 1700  
San Diego, CA 92101  
Tel: (619) 338-1100  
Fax: (619) 338-1101  
tblood@bholaw.com

Richard L. Coffman

TX Bar No. 04497460  
(*Pro hac vice* to be filed)

**THE COFFMAN LAW FIRM**

First City Building

505 Orleans St., Fifth Floor  
Beaumont, TX 77701  
Tel: (409) 833-7700  
Fax: (866) 835-8250  
rcoffman@coffmanlawfirm.com

Brandee J.K. Faria  
HI Bar No. 6970  
(*Pro hac vice* to be filed)  
**PERKIN & FARIA, LLC**  
841 Bishop Street, Suite 1000  
Honolulu, HI 96813  
Tel: (808) 523-2300  
Fax: (808) 697-5302  
info@perkinlaw.com

Charles T. Lester, Jr.  
OH Bar No. 0017601  
(*Pro hac vice* to be filed)  
**CHARLES T. LESTER, JR.,**  
**ATTORNEY AT LAW**  
P.O. Box 75069  
Fort Thomas, KY 41075-0069  
Tel: (859) 838-4294, (859) 781-2406  
Fax: (859) 486-6590  
charles@lawbylester.com

Mark K. Gray  
KY Bar No. 83552  
(*Pro hac vice* to be filed)  
**GRAY & WHITE**  
713 E. Market St., Suite 200  
Louisville, KY 40202  
Tel: (502) 805-1800  
Fax: (502) 618-4059  
mgray@grayandwhitelaw.com

Ralph K. Phalen



MO Bar No. 36687  
(*Pro hac vice* to be filed)  
**RALPH K. PHALEN LAW, P.C.**  
4310 Madison  
Suite 140  
Kansas City, MO 64111  
Tel: (816) 589-0753  
Fax: (816) 471-1701  
phalenlaw@yahoo.com

Kevin B. Rogers  
IL Bar No. 6192609  
(*Pro hac vice* to be filed)  
**LAW OFFICES OF KEVIN ROGERS**  
307 North Michigan Avenue  
Suite 305  
Chicago, IL 60601  
Tel: (312) 332-1188  
Fax: (312) 332-0192  
kevinrogerslaw@gmail.com

Edward K. O'Brien  
NH Bar No. 2866  
(*Pro hac vice* to be filed)  
**O'BRIEN LAW FIRM, P.C.**  
One Sundial Avenue  
5th Floor  
Manchester, NH 03103  
Tel: (603) 668-0600  
Fax: (603) 672-3815  
eobrien@ekoblaw.com

**CERTIFICATE OF SERVICE**

I hereby certify that on this date I electronically filed the foregoing **AMENDED CLASS ACTION COMPLAINT** with the Clerk of Court using the CM/ECF system which will automatically send email notification of such filing to the attorneys of record.

Dated: September 25, 2017

/s/ David J. Worley  
David J. Worley